Development of Attack Scenarios Against The Air Transportation System

Michael Sorokach[1], Sherilyn Brown[1], Kenneth Fisher[2],
Frank Jones[1], Terry Bott[3,5], Stephen Eisenhawer[3,5],
John Foggia[4] and Joseph Santos[4]

MODSIM World Conference and Expo 2007
Virginia Beach, VA

September 13, 2007

[1]NASA Langley Research Center, Hampton VA
[2]NASA Glenn Research Center, Cleveland OH
[3]Logic Evolved Technologies, Santa Fe NM
[4]National Institute of Aerospace, Hampton VA
[5]Los Alamos National Laboratory, Los Alamos NM

- **Problem**: Estimating the risk of terrorism to a system depends upon the range of attack scenarios available to the adversary.

- **Approach**: Use logic gate trees (LGTs) to represent subject matter expert (SME) knowledge in a model that provides the basis for the risk analysis. The LGTs are developed using the Logic Evolved Decision (LED) methodology.

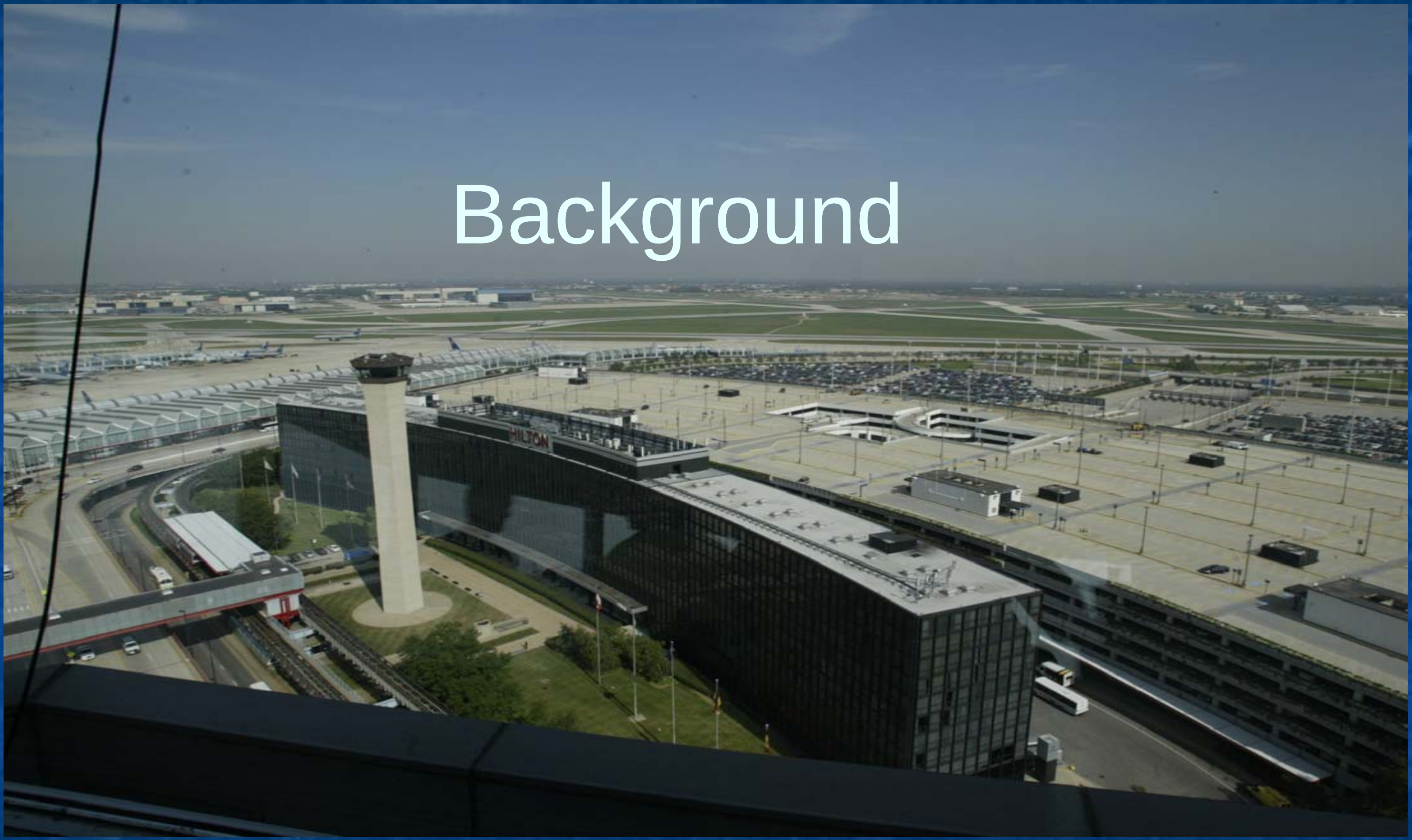
Presentation Outline

- Background
- Structure of a Terrorist Attack
- LED Models for the Air Transportation System (ATS)
- Scenario Groupings, Concept of Operations (CONOPS), and Technology Insertions
- The Role of Expert Elicitation
- Conclusions

NASA

LOGIC EVOLVED TECHNOLOGIES

Background



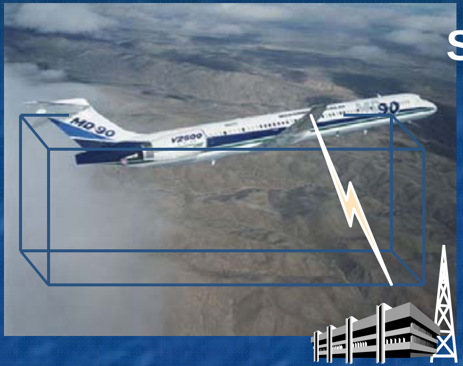
NIA NATIONAL INSTITUTE OF AEROSPACE

Los Alamos

Risk-based Prioritization of NASA Aviation Security Research

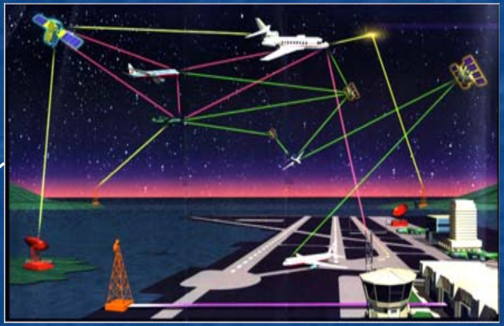
- NASA Goal:
  - **Use a *top-down analysis* approach to rank order security technology investments**
- Objective:
  - **Decision support tool to prioritize aviation security research**
  - **Based upon an air transportation system (ATS) risk assessment**
- Technical Challenges:
  - **Pioneering development effort**
  - **Security assessments for the entire ATS**
  - **Extensive integration of subject matter experts**

Approach to Aviation Security

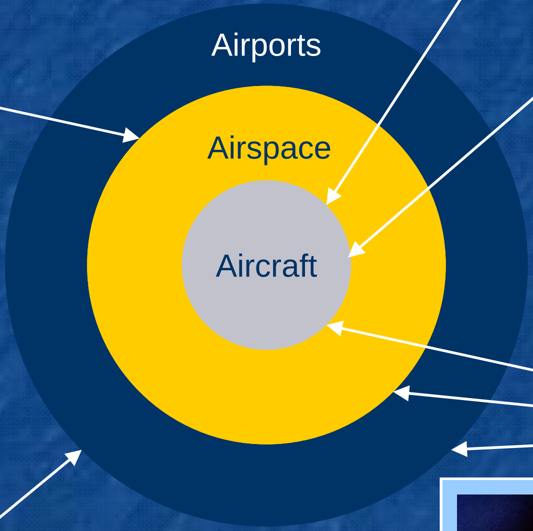


Secure and protect the aircraft

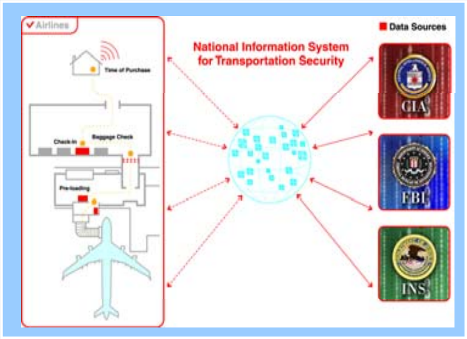
Harden the National Airspace System



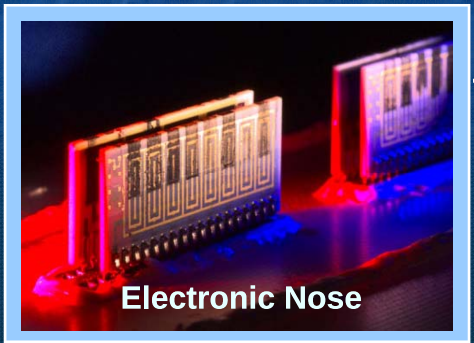
Secure vehicle CNS systems



Integrate advanced sensors throughout the system

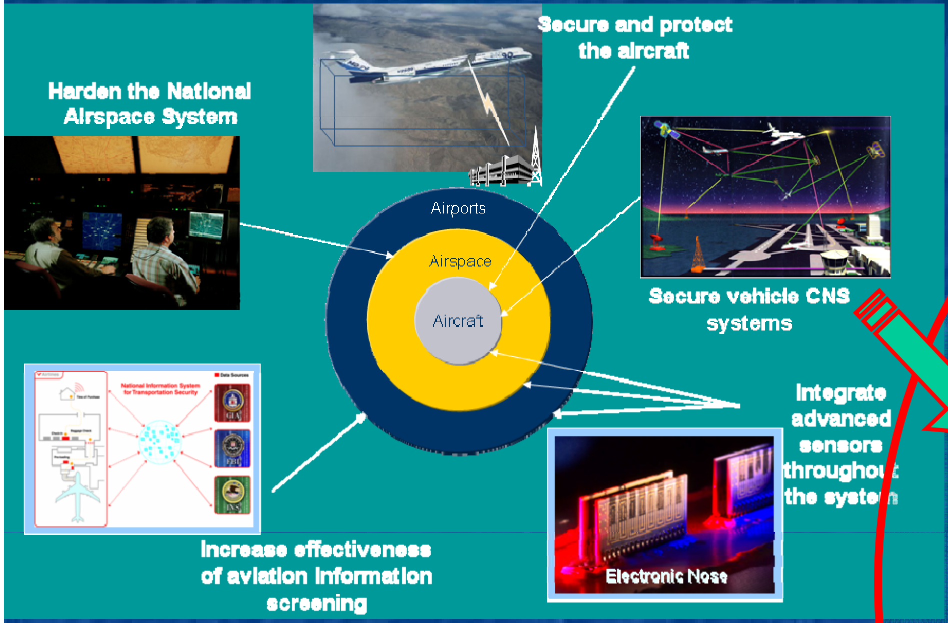


Increase effectiveness of aviation information screening



Electronic Nose

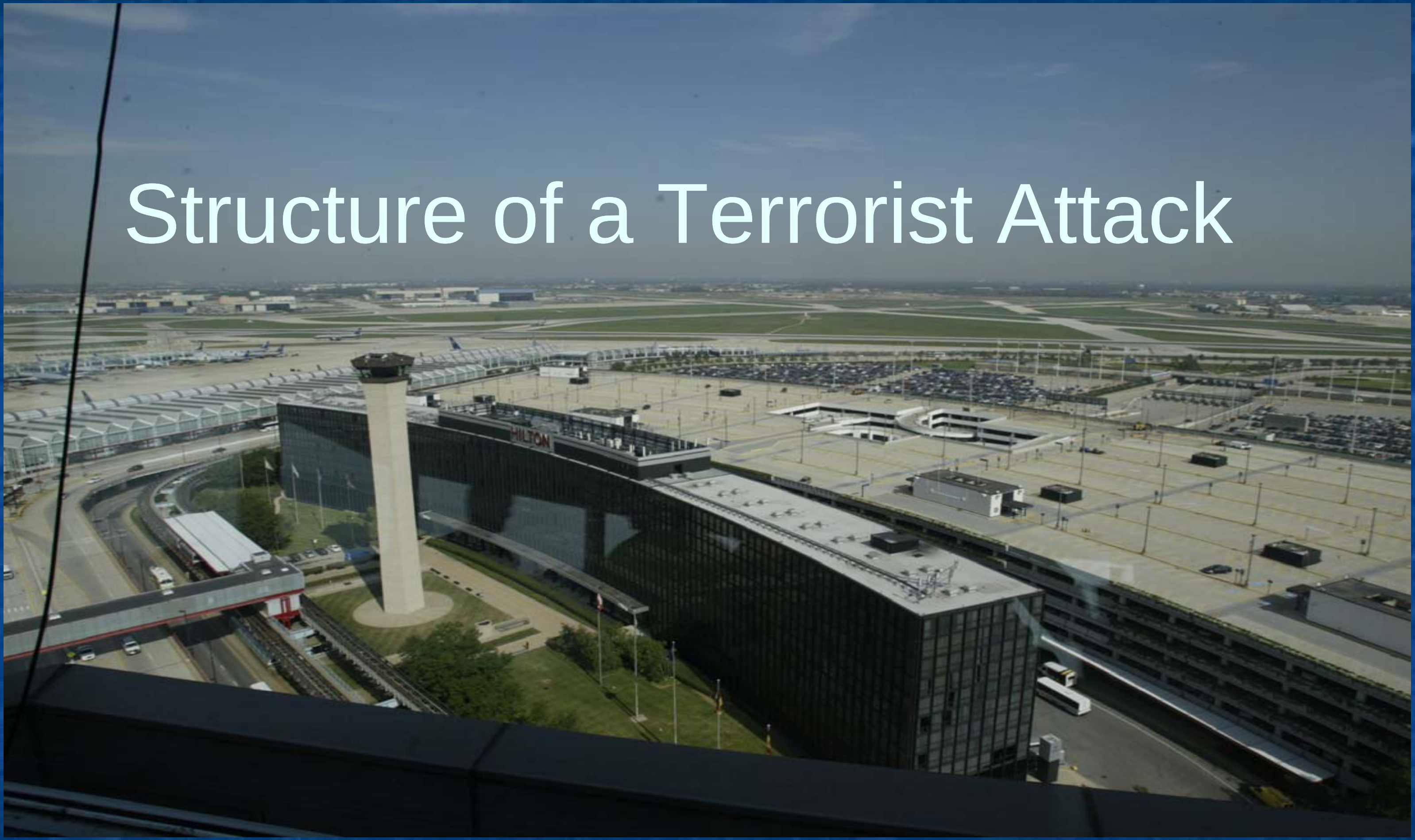
Assessing Air Transportation System Risk


Secure and protect the aircraft
Harden the National Airspace System
Airports
Airspace
Aircraft
Secure vehicle CNS systems
Integrate advanced sensors throughout the system
Increase effectiveness of aviation information screening
Electronic Nose

Risk Assessment Approach to Aviation Security

- ATS Divided into Three Sub-systems
- Aircraft Further Decomposed into Federal Aviation Regulation Parts
  - **Aircraft**
    - Part 121 Passenger/Cargo
    - Part 121 All Cargo
    - Part 135
    - Part 91
  - **Airport**
  - **Airspace**

Structure of a Terrorist Attack



An Attack Scenario Is A Process

*Description of the **process** an adversary carries out operations against a **target***

Target Selection → Planning → Logistics → Assault → Target Response

Attacker

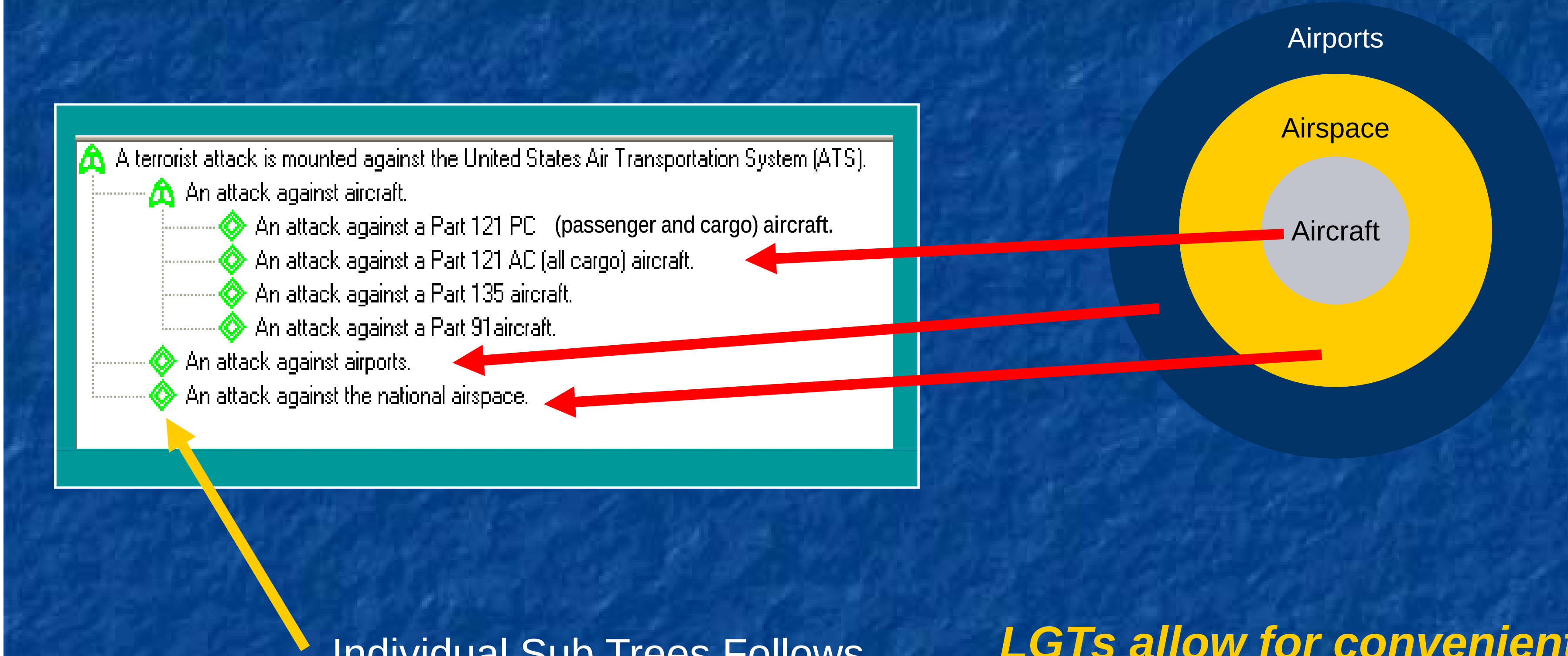
For the ATS a very large number of scenarios are possible

LED Models for the ATS

Possible Scenarios Are Generated Using LGTs with LED

1. **Develop a Possibility Tree**
   - Composed of elements of a process
   - Logical operators (i.e., *and* / *or*) connect elements
   - Deduction facilitates capturing a large set of possible scenarios
2. **Solve the Possibility Tree**
   - Generate scenarios from logically linked elements
   - Prune the tree to develop a spanning set of scenarios

Logic Gate Tree for Attacks against the ATS

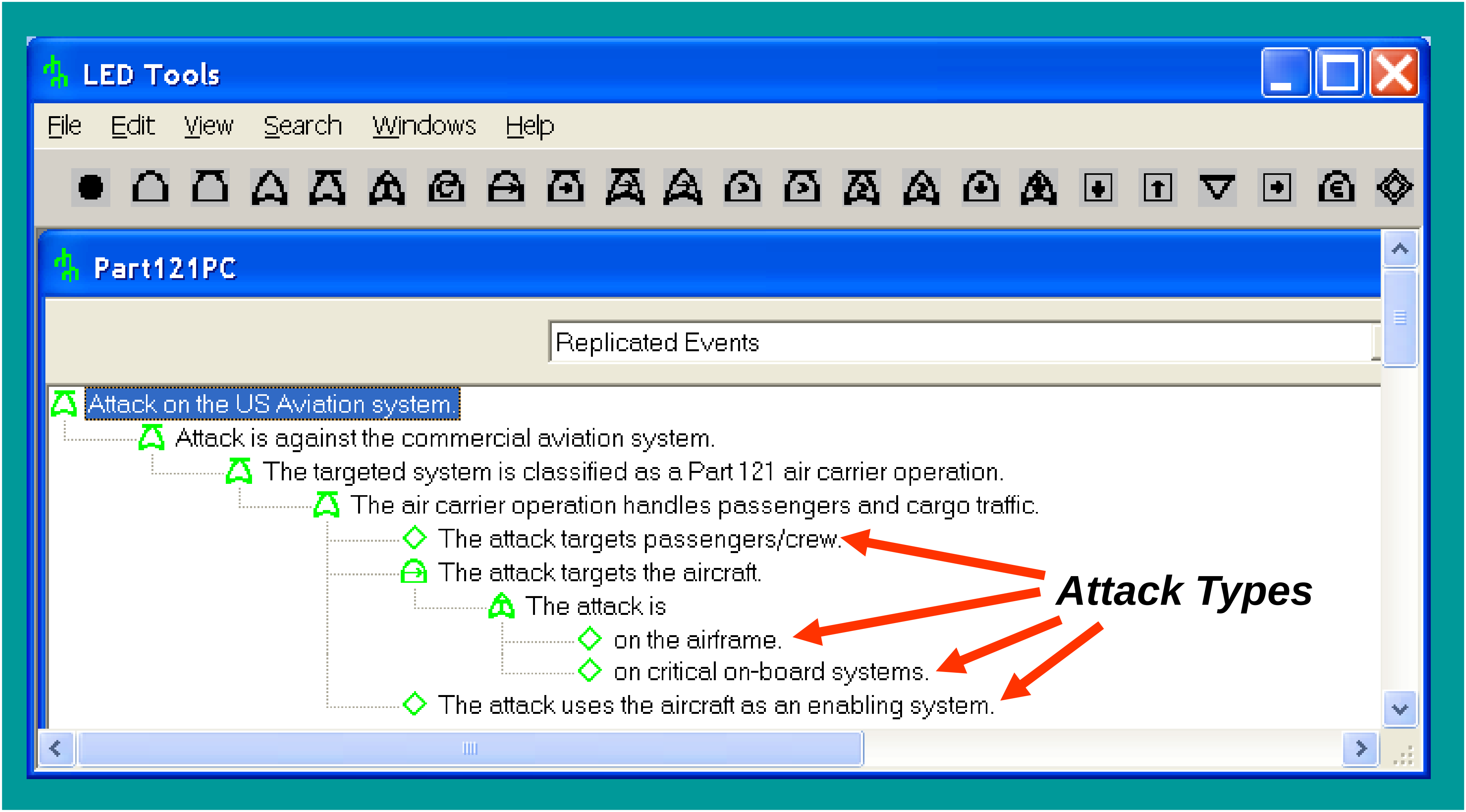


- A terrorist attack is mounted against the United States Air Transportation System (ATS).
  - An attack against aircraft.
    - An attack against a Part 121 PC (passenger and cargo) aircraft.
    - An attack against a Part 121 AC (all cargo) aircraft.
    - An attack against a Part 135 aircraft.
    - An attack against a Part 91 aircraft.
  - An attack against airports.
  - An attack against the national airspace.

Individual Sub Trees Follows Logical Decomposition

LGTs allow for convenient modularization of the attack space

Possibility Tree for Part 121 PC Attack Scenarios



Replicated Events

- Attack on the US Aviation system.
  - Attack is against the commercial aviation system.
    - The targeted system is classified as a Part 121 air carrier operation.
      - The air carrier operation handles passengers and cargo traffic.
        - The attack targets passengers/crew.
        - The attack targets the aircraft.
          - The attack is
            - on the airframe.
            - on critical on-board systems.
        - The attack uses the aircraft as an enabling system.

Attack Types

The Possibility-Tree Solution Gives a Comprehensive Set of Attack Scenarios

Attack on the US aviation system. Attack is against the commercial aviation system. The targeted system is classified as a Part 121 air-carrier operation. The air-carrier operation handles passenger and cargo traffic. The attack targets the aircraft. The attack is on the airframe. The attack originates external to the aircraft. The attack involves weaponry. The weapon used is a man-portable missile. The attacker acquires the weapon system. The attacker transports the missile system to the attack site. The attacker acquires the target. The attacker fires the missile. The missile flies to the target. The missile warhead detonates. The attacker group consists of outsiders only.

Attack scenarios appear in natural language form for use with SMEs

Scenario Groupings, CONOPS, and Technology Insertions

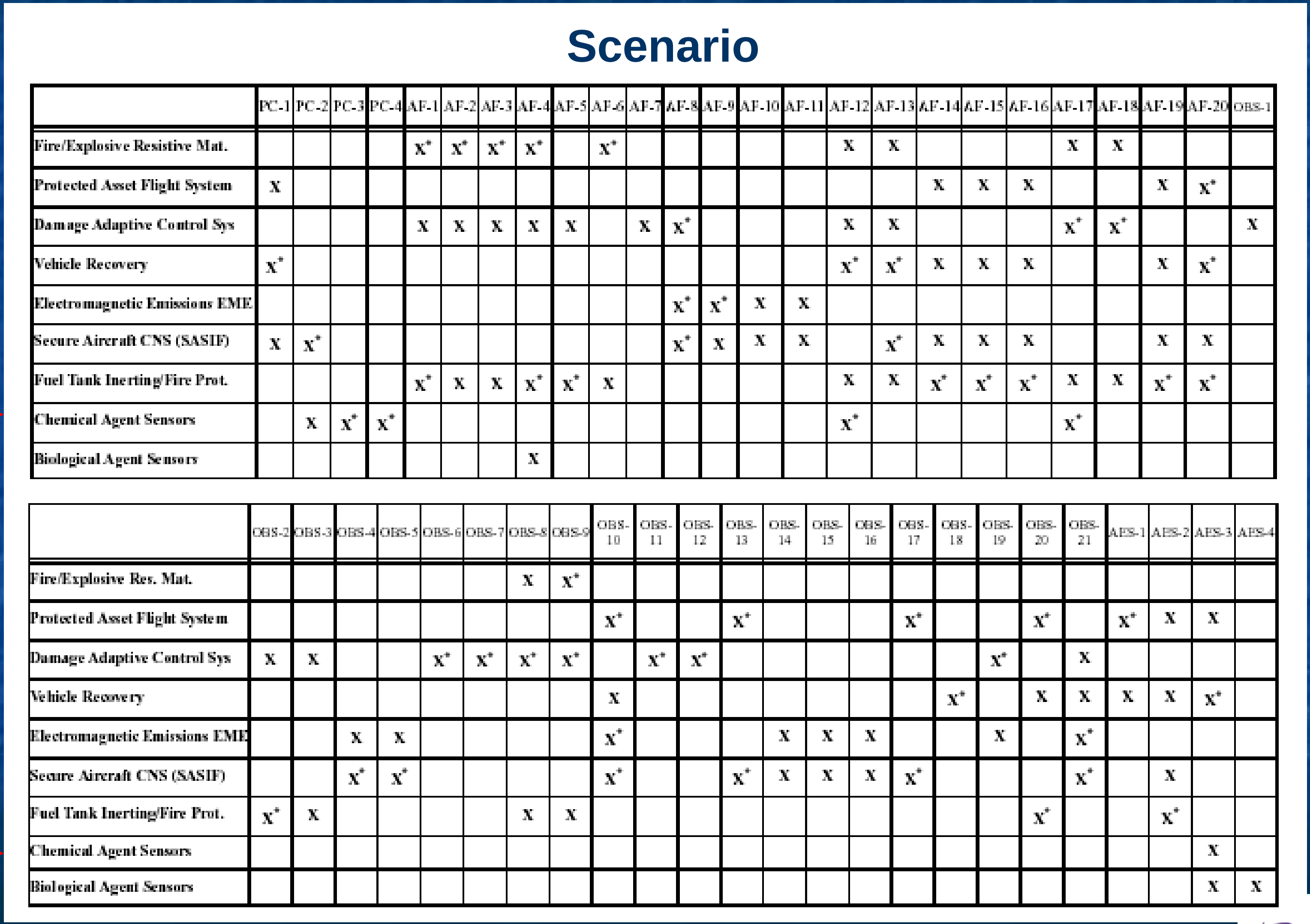
Summary Attack Scenarios in Spanning Set for Part 121 PC Aircraft

Type of Attack	Number of Scenarios	Example
Attack on crew or passengers	4	Dispersion of chemical agent in passenger compartment
Attack on airframe	20	Missile attack with man-portable system
Attack on critical on-board systems	24	Jamming or spoofing of navigational aids
Use of aircraft as an enabling system for weapons-of-mass-destruction attack	4	Variations of 9/11 World Trade Center attack

Screening process for developing a workable sub-set of scenarios that are representative of a larger class of attacks.

Similar spanning sets were developed for airports and the air space in consultation with SMEs

A Scenario / Technology Crosswalk



Scenario

Technology

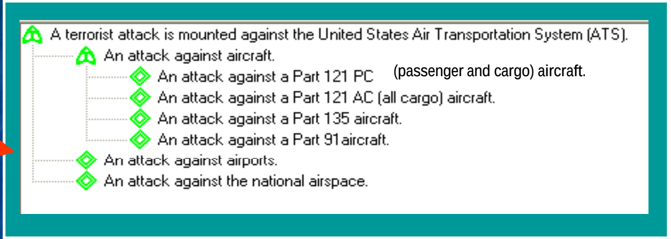
	PC-1	PC-2	PC-3	PC-4	AF-1	AF-2	AF-3	AF-4	AF-5	AF-6	AF-7	AF-8	AF-9	AF-10	AF-11	AF-12	AF-13	AF-14	AF-15	AF-16	AF-17	AF-18	AF-19	AF-20	OBS-1
Fire/Explosive Resistive Mat.					x*	x*	x*	x*		x*						x	x				x	x			
Protected Asset Flight System	x																	x	x	x			x	x*	
Damage Adaptive Control Sys					x	x	x	x	x		x	x*				x	x				x*	x*			x
Vehicle Recovery	x*															x*	x*	x	x	x			x	x*	
Electromagnetic Emissions EME												x*	x*	x	x										
Secure Aircraft CNS (SASIF)	x	x*										x*	x	x	x		x*	x	x	x			x	x	
Fuel Tank Inerting/Fire Prot.					x*	x	x	x*	x*	x						x	x	x*	x*	x*	x	x	x*	x*	
Chemical Agent Sensors		x	x*	x*												x*					x*				
Biological Agent Sensors								x																	

Technology

	OBS-2	OBS-3	OBS-4	OBS-5	OBS-6	OBS-7	OBS-8	OBS-9	OBS-10	OBS-11	OBS-12	OBS-13	OBS-14	OBS-15	OBS-16	OBS-17	OBS-18	OBS-19	OBS-20	OBS-21	AES-1	AES-2	AES-3	AES-4
Fire/Explosive Res. Mat.							x	x*																
Protected Asset Flight System									x*			x*				x*			x*		x*	x	x	
Damage Adaptive Control Sys	x	x			x*	x*	x*	x*		x*	x*							x*		x				
Vehicle Recovery									x								x*		x	x	x	x	x*	
Electromagnetic Emissions EME			x	x					x*				x	x	x			x		x*				
Secure Aircraft CNS (SASIF)			x*	x*					x*			x*	x	x	x	x*				x*		x		
Fuel Tank Inerting/Fire Prot.	x*	x					x	x											x*			x*		
Chemical Agent Sensors																							x	
Biological Agent Sensors																							x	x

Concept of Operations for Technologies

- **Technology CONOPS**
  - **CONOPS processes converted into LED trees**
  - **Define technology insertion points**
  - **Operations are fine-tuned**
  - **Gaps and functional requirements result**
  - **Define how the overall system functions**
  - **Discover technology interactions, gaps, and system impacts**
  - **Identify responsibilities and information transfers between system components**



- A terrorist attack is mounted against the United States Air Transportation System (ATS).
  - An attack against aircraft.
    - An attack against a Part 121 PC (passenger and cargo) aircraft.
    - An attack against a Part 121 AC (all cargo) aircraft.
    - An attack against a Part 135 aircraft.
    - An attack against a Part 91aircraft.
  - An attack against airports.
  - An attack against the national airspace.

- **CONOPS based system requirements for technologies**
  - **Define and optimize system operating parameters**

The Role of Expert Elicitation

Many Different Types of SMEs Participated in the Analysis

- National Institute of Aerospace (NIA)
  - Aviation System Expert Consultants
- Aviation Operations
  - Pilots
  - Airport Managers
  - Air Traffic Controllers
- Air Force Research Laboratory (AFRL)
  - Electromagnetic Effects Expertise
- NASA Aviation Security Research Projects
  - Research Project Input to Analysis
- Volpe Center Department of Transportation (Volpe)
  - Cost/Benefit Studies
- Experts on terrorism from various agencies

SME Roles

- Definition of system for analysis
- Development of attack scenario possibility trees
- Selection of spanning sets
- Revision of trees and sets based upon initial risk assessment
- Development of CONOPS and identification of technology insertion points

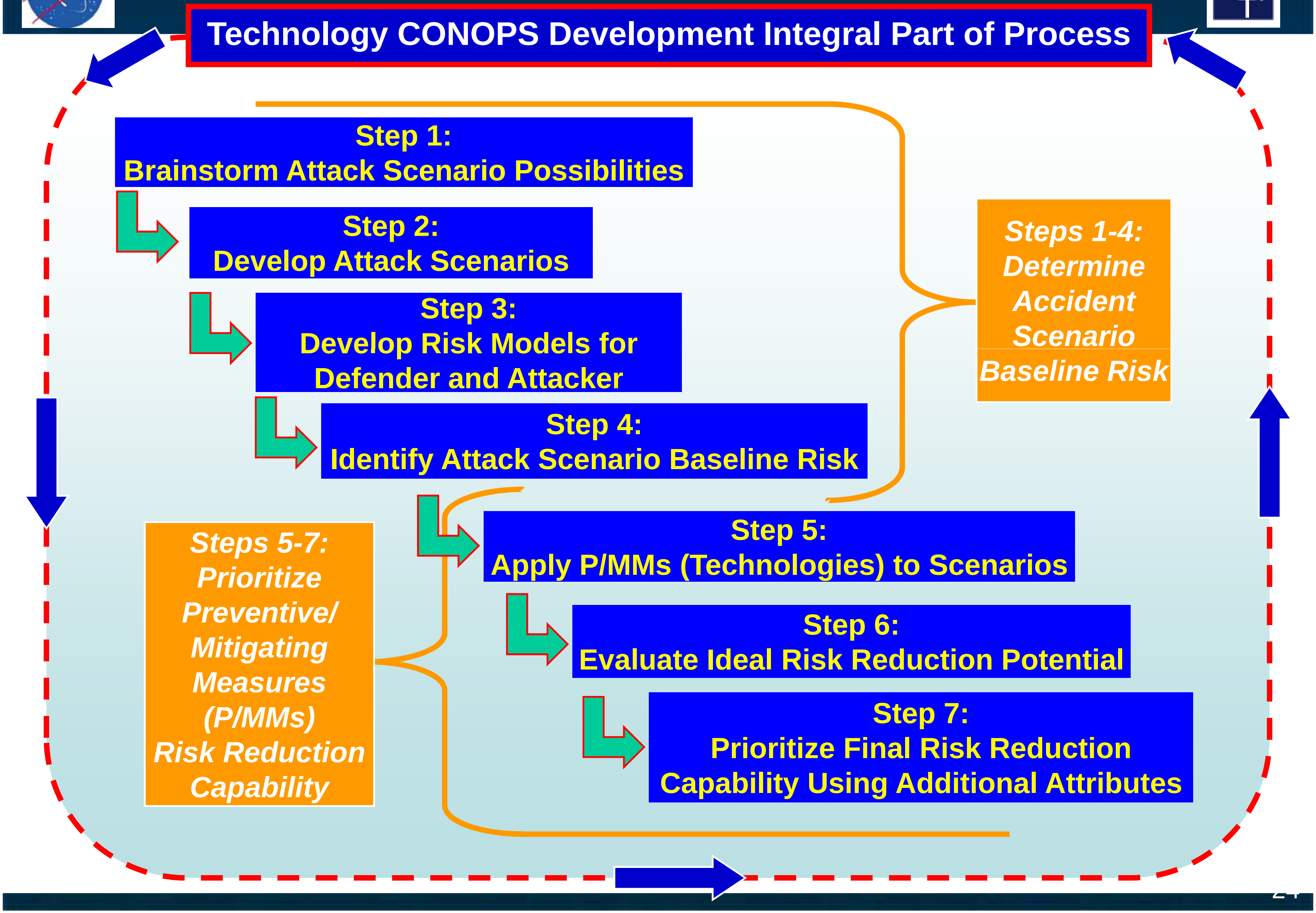
Conclusions

- To be meaningful, terrorist risk analyses must have a well-defined set of attack scenarios
  - Logic gate trees provide a structured approach to scenario development
  - The possibility tree contains a very large set of scenarios
  - Spanning sets can be developed for different purposes
- An LGT model can be extended to incorporate CONOPS and to help define technology requirements
- Terrorist risk analysis is highly dependent on SME knowledge
  - Possibility trees are an efficient way to integrate large amounts of expert knowledge
  - A tree can be easily updated to reflect new information or modified as a result of SME interactions

Backup

Detailed Risk Assessment Process for Prioritizing NASA Research in Aviation Security

Aviation Security Risk Assessment 7 Step Development Process



Technology CONOPS Development Integral Part of Process

Step 1:
Brainstorm Attack Scenario Possibilities

Step 2:
Develop Attack Scenarios

Step 3:
Develop Risk Models for Defender and Attacker

Step 4:
Identify Attack Scenario Baseline Risk

Steps 1-4: Determine Accident Scenario Baseline Risk

Step 5:
Apply P/MMs (Technologies) to Scenarios

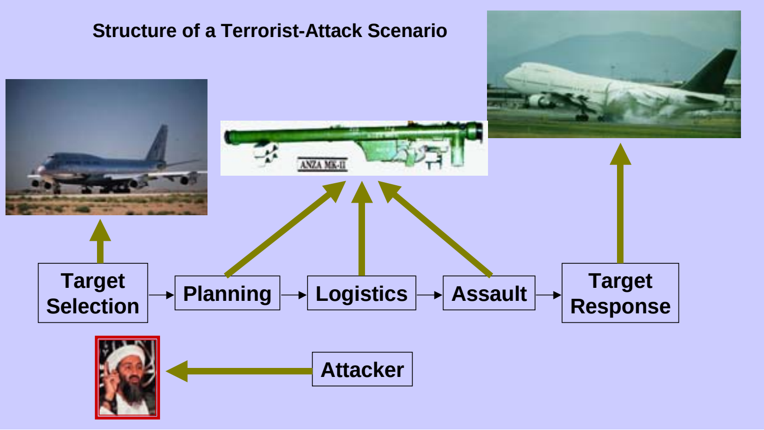
Step 6:
Evaluate Ideal Risk Reduction Potential

Step 7:
Prioritize Final Risk Reduction Capability Using Additional Attributes

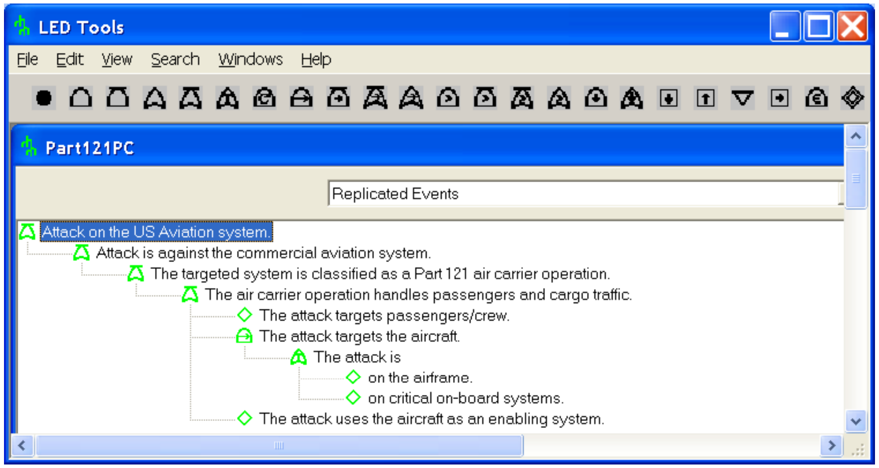
Steps 5-7: Prioritize Preventive/ Mitigating Measures (P/MMs) Risk Reduction Capability

ATS Risk Assessment Development Process

Step 1: Think Like a Terrorist

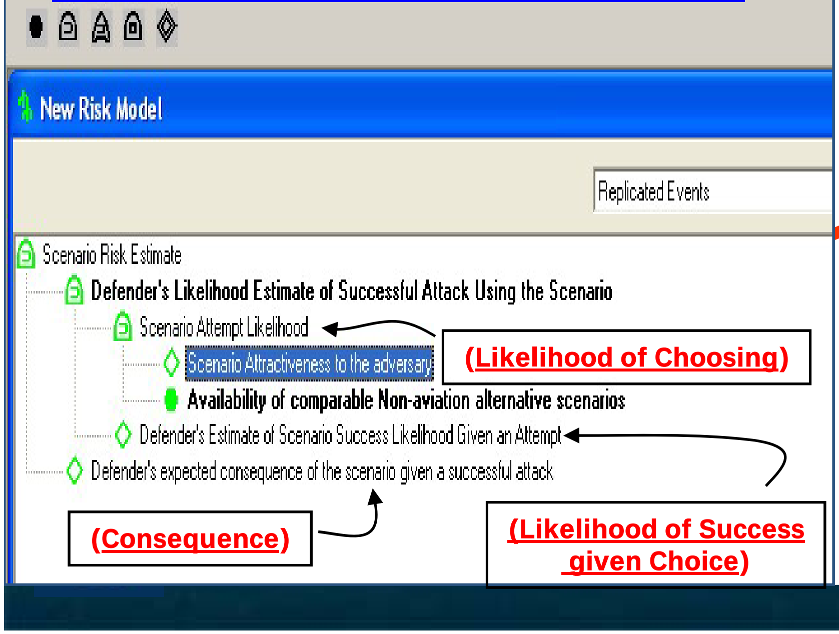


Step 2: Develop Attack Scenarios



- Attack on the US Aviation system.
  - Attack is against the commercial aviation system.
    - The targeted system is classified as a Part 121 air carrier operation.
      - The air carrier operation handles passengers and cargo traffic.
        - The attack targets passengers/crew.
        - The attack targets the aircraft.
          - The attack is
            - on the airframe.
            - on critical on-board systems.
        - The attack uses the aircraft as an enabling system.

Step 3: Develop Risk Models for Defender and Attacker



- Scenario Risk Estimate
  - Defender's Likelihood Estimate of Successful Attack Using the Scenario
    - Scenario Attempt Likelihood
      - Scenario Attractiveness to the adversary
      - Availability of comparable Non-aviation alternative scenarios
    - Defender's Estimate of Scenario Success Likelihood Given an Attempt
  - Defender's expected consequence of the scenario given a successful attack

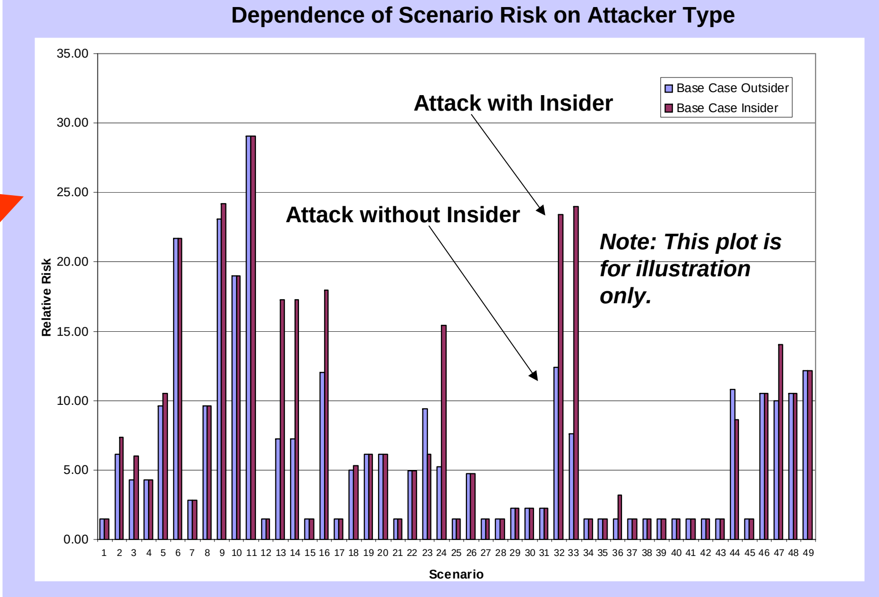
(Likelihood of Choosing)

(Consequence)

(Likelihood of Success given Choice)

Step 4: Identify Attack Scenario Baseline Risk

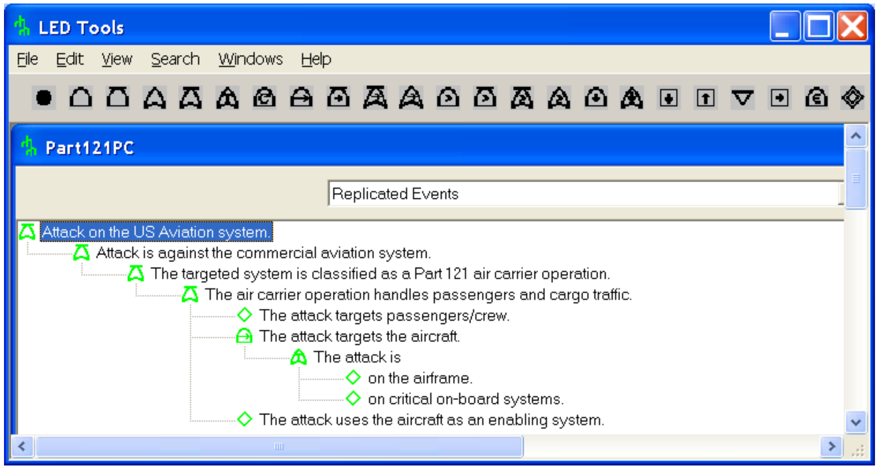
Dependence of Scenario Risk on Attacker Type



Note: This plot is for illustration only.

The Possibility Tree Solution Gives a Comprehensive Set of Attack Scenarios

Step 2 Details:
Attack Scenario Development Using LED Approach



- Attack on the US Aviation system.
  - Attack is against the commercial aviation system.
    - The targeted system is classified as a Part 121 air carrier operation.
      - The air carrier operation handles passengers and cargo traffic.
        - The attack targets passengers/crew.
        - The attack targets the aircraft.
          - The attack is
            - on the airframe.
            - on critical on-board systems.
        - The attack uses the aircraft as an enabling system.

Attack on the US aviation system. Attack is against the commercial aviation system. The targeted system is classified as a Part 121 air-carrier operation. The air-carrier operation handles passenger and cargo traffic. The attack targets the aircraft. The attack is on the airframe. The attack originates external to the aircraft. The attack involves weaponry. The weapon used is a man-portable missile. The attacker acquires the weapon system. The attacker transports the missile system to the attack site. The attacker acquires the target. The attacker fires the missile. The missile flies to the target. The missile warhead detonates. The attacker group consists of outsiders only.

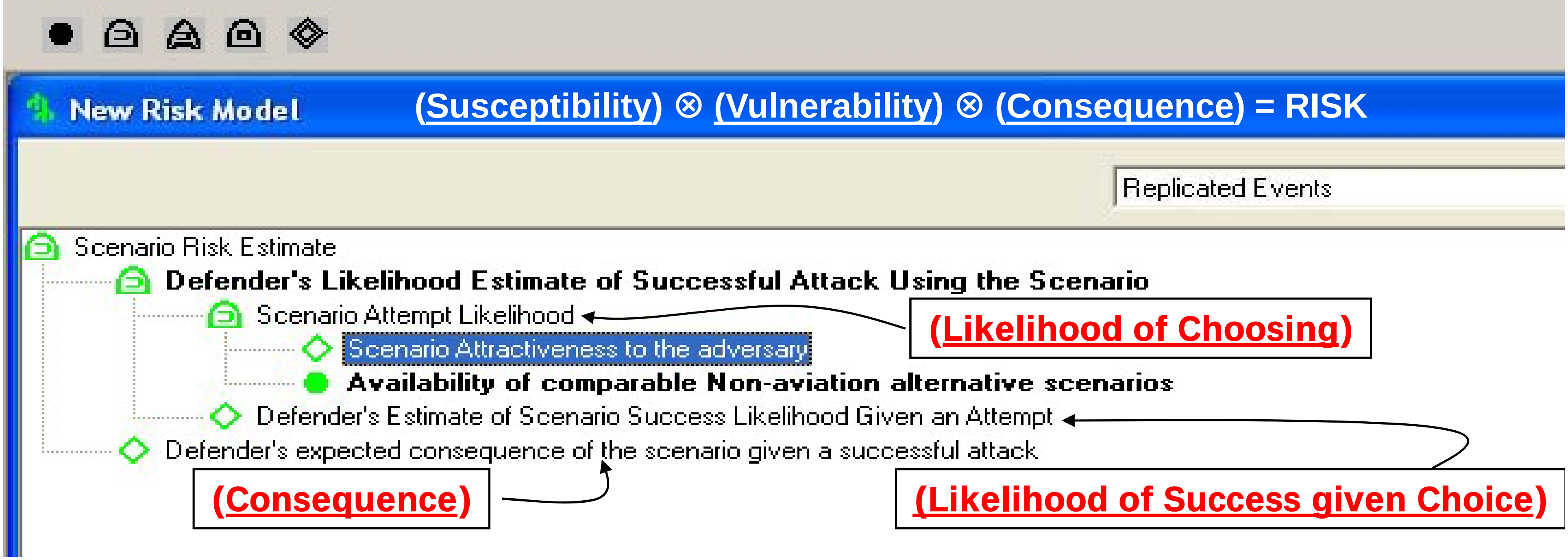
Step 3 Details: Inferential Risk Model Development

Security RISK … of a Scenario or Attack must account for INTENT

(<u>Likelihood of Choosing</u>) ⊗ (<u>Likelihood of Success given Choice</u>) ⊗ (<u>Consequence</u>) = RISK

- Recognizes Factors Contributing to Risk
- Logical Operators (i.e., *and* / *or*) Connect Factors
- In lieu of Reasonable Probabilities, Risk is Inferred by Chaining Rule Bases According to Model Logic Using:

  Linguistic Variables - Approximate Reasoning - Fuzzy Membership Sets



New Risk Model (<u>Susceptibility</u>) ⊗ (<u>Vulnerability</u>) ⊗ (<u>Consequence</u>) = RISK

Replicated Events

- Scenario Risk Estimate
  - **Defender's Likelihood Estimate of Successful Attack Using the Scenario**
    - Scenario Attempt Likelihood
      - Scenario Attractiveness to the adversary
      - **Availability of comparable Non-aviation alternative scenarios**
    - Defender's Estimate of Scenario Success Likelihood Given an Attempt
  - Defender's expected consequence of the scenario given a successful attack

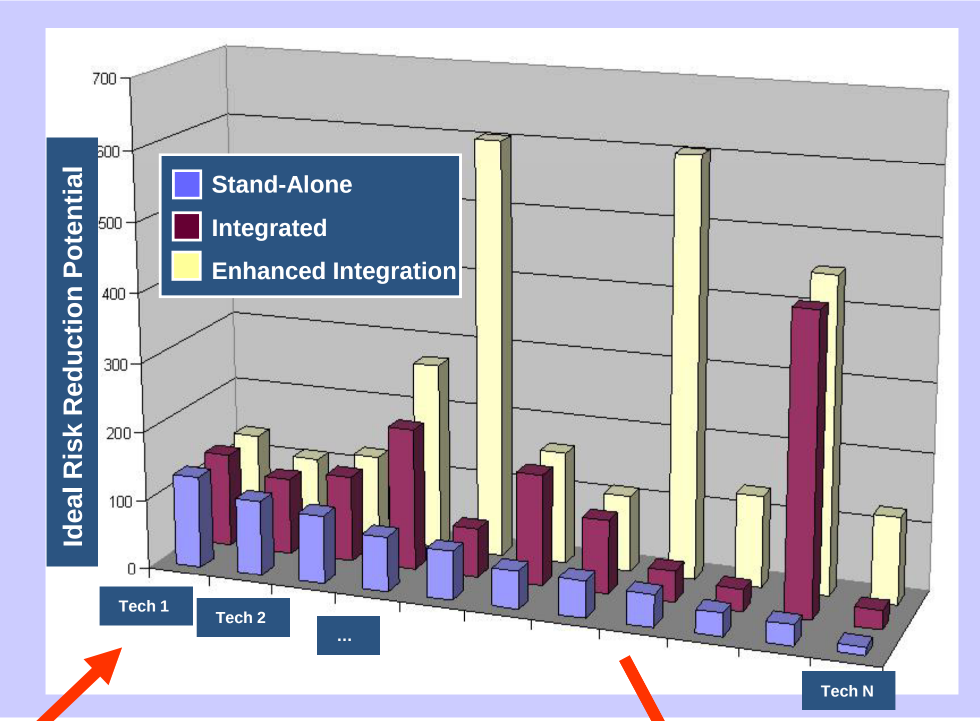
(<u>Likelihood of Choosing</u>)

(<u>Consequence</u>)

(<u>Likelihood of Success given Choice</u>)

Aviation Security Research Portfolio Prioritization

Step 6: Prioritize Ideal Risk Reduction Potential



Step 5: Map Technologies to Scenarios

Prioritizing Aviation Security Research

Identify a spanning set of possible scenarios

Map the PM suites onto the possible scenario set

Preventive/Mitigating Measure Suite

Scenarios Addressed

Technologies Evaluated for Three Categories

- Stand-Alone
- Integrated
- Enhanced Integration

End State Achieved:

-Technologies Prioritized Based Upon a Comprehensive Risk Assessment.

Results In:

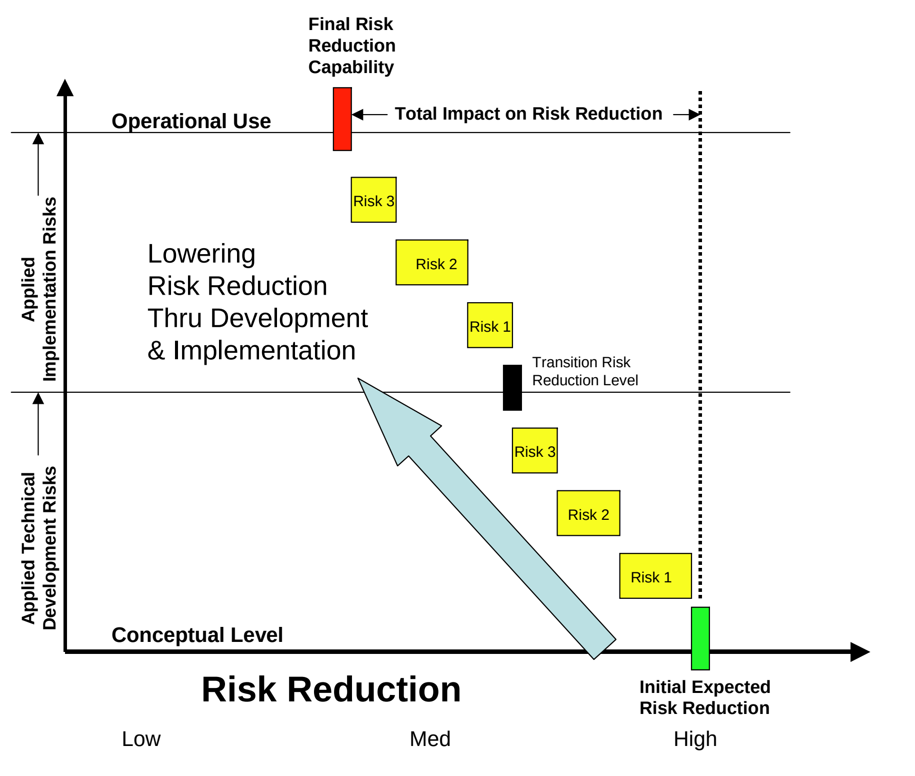
1) Technologies Prioritized Based on Risk Reduction Potential for Three Levels of Integration

2) Risk Assessment for ATS

Step 7: Prioritize Final Risk Reduction Capability

Additional Prioritization Attributes:

- Ideal Risk Reduction Potential ➔ **Input**
- Costs
  - **Development**
  - **Operating**
  - **Capital**
  - **Consequence**
- Benefit
- Technical Risk
  - **Technology development**
  - **Dependencies**
  - **Complexity**
- Implementation Risk
  - **Certification**
  - **Cultural issues**
  - **User acceptance**
- Technology Readiness Level
- Cost
  - **Funding available for technology development**
- Schedule
  - **Time available for technology development**
- National Needs Based Time Frame for Technology Development
- Technology Impact on Throughput Volume
  - Delay introduced by technology insertion
  - Technology impact on demand
  - Technology impact on capacity



Final Risk Reduction Capability
Operational Use
Total Impact on Risk Reduction
Applied Implementation Risks
Risk 3
Risk 2
Risk 1
Lowering Risk Reduction Thru Development & Implementation
Transition Risk Reduction Level
Applied Technical Development Risks
Risk 3
Risk 2
Risk 1
Conceptual Level
Risk Reduction
Initial Expected Risk Reduction
Low
Med
High